Examen Final – Communications quantiques

June 9, 2018

Durée: 1h30

Questions de cours

En cryptographie, le protocole BB84 est le premier mécanisme d'échange de clé quantique a avoir été formalisé, et en fait le premier protocole de cryptographie quantique. Il a été proposé en 1984 par Charles Bennett et Gilles Brassard.

1. Pour ce protocole, indiquez l'information échangée entre Alice et Bob sur un canal privé et qui est envoyée sur un canal public. Dans chaque cas, indiquez si le canal doit être un canal quantique ou peut être un canal classique.

2. Donner deux techniques d'espionnage (dites attaques) qui menacent le BB84.

3. Donner une implémentation schématique de BB84 en indique les trois étapes importantes au cours de l'échange de la clé.

4. Quelle sont les sources de bruit qu'il devient possible pour Eve de passer inaperçue? (comment?).

Exercice (Cloning Attack)

Alice envoie un photon dans un état quantique $|\phi_A\rangle$. Eve va créer un clone de chaque photon transmis et renvoie un photon a Bob. Remarquons que Eve n'a pas encore fait de mesure et n'a donc pas choisi de base. Ensuite, Alice et Bob se communiquent leurs bases et ne gardent que celles qu'ils ont en commun. Eve, ayant écoute cela, peut donc choisir à chaque fois la bonne base pour mesurer ses photons, ce qui représente déjà un gros avantage par rapport à l'attaque Intercept-Resend.
La meilleure transformation unitaire de clonage est

$$U : \mathcal{E}_{AE} \to \mathcal{E}_{AE}$$

définie par

$$\begin{aligned} U|0\rangle_{y,A}|0\rangle_{y,E} &= |0\rangle_{y,A}|0\rangle_{y,E} \\ U|1\rangle_{y,A}|0\rangle_{y,E} &= \cos(\theta)|1\rangle_{y,A}|0\rangle_{y,E} + \sin(\theta)|0\rangle_{y,A}|1\rangle_{y,E} \end{aligned}$$

où $\theta \in \left[0, \frac{\pi}{2}\right]$.
En effectuant des changements des bases, calculer les informations conditionnelles et mutuelle et déterminer leurs limites, entre Alice et Bob et entre Alice et Eve.